UNIT 1.

1.What is WSN, energy scavenging. explain in detail.

Wireless sensor networks (WSN) are networks of small, low-power devices that are equipped with sensors and wireless communication capabilities. These devices are used to collect and transmit data about the environment, such as temperature, humidity, and motion.

Energy scavenging, also known as energy harvesting, is a technique used to power these devices without the need for traditional batteries. Instead, energy scavenging devices gather small amounts of energy from the environment, such as from sunlight, vibrations, or thermal gradients, and convert it into usable electrical power. This allows the devices to operate indefinitely, as long as there is a source of energy available.

There are a variety of different energy scavenging techniques that can be used in WSNs, including:

Solar energy: Photovoltaic cells are used to convert sunlight into electrical power.

Thermal energy: Devices such as thermoelectric generators can convert temperature differences into electrical power.

Kinetic energy: Devices such as piezoelectric generators can convert mechanical vibrations into electrical power.

Chemical energy: Devices such as fuel cells can convert chemical energy into electrical power.

Overall, energy scavenging is an important technique for extending the lifetime of WSN devices and enabling them to operate in remote or hard-to-reach locations where traditional batteries would be difficult to replace.

2.Relationship between computation and communication in detail in adhoc

In ad-hoc networks, the relationship between computation and communication is even more crucial as the devices are mobile and have limited energy resources. The balance between computation and communication can have a significant impact on the energy efficiency and overall performance of the network.

In ad-hoc networks, computation is typically performed by the nodes to process and analyze the data they have collected. This could include tasks such as filtering, compression, aggregation, or machine learning algorithms. The more computation that is performed by each node, the less data needs to be transmitted over the network, which can help to conserve energy. However, if the computation is too complex or too resource-intensive, it can consume a significant amount of energy and impact the overall performance of the network.

On the other hand, communication is used to share data and information between the nodes in the network. This could include tasks such as routing, data dissemination, or multicast. The more communication that is required, the more energy is consumed by the nodes. To reduce the energy consumption, the communication should be minimized by reducing the number of transmissions or by using more efficient communication protocols.

Finding the right balance between computation and communication is a challenging task in ad-hoc networks, and it depends on the specific application, network topology, and energy constraints. In general, a good ad-hoc network design should aim to minimize the amount of communication while still providing sufficient computation to meet the requirements of the application.

3.What are sensor nodes? Explain in detail with example

Sensor nodes, also known as motes, are small, low-power devices that are used in wireless sensor networks (WSNs) to collect and transmit data about the environment. They typically consist of a microcontroller, one or more sensors, a wireless communication module, and a power source. The sensor nodes are capable of sensing environmental conditions and sending data to a central location for analysis.

A sensor node typically includes the following components:

Microcontroller: A small computer that controls the operation of the sensor node and manages the data it collects.

Sensors: Devices that measure environmental conditions, such as temperature, humidity, light, and motion.

Wireless communication module: Allows the sensor node to communicate with other nodes in the network and send data to a central location.

Power source: Typically a battery, but some sensor nodes are designed to be powered by energy scavenging techniques such as solar or kinetic energy.

An example of sensor nodes is a network of temperature sensors that are placed in a warehouse to monitor the temperature and humidity. The sensor nodes collect data from the environment and send it to a central location where it can be analyzed and used to optimize the warehouse's temperature and humidity control systems.

Another example is a network of motion sensors that are placed in a public park to monitor foot traffic and help city officials plan for future events and maintenance. The sensor nodes detect motion and send the data to a central location where it can be analyzed and used to plan for future events and maintenance.

Overall, sensor nodes are a key component of WSNs that allow for the collection of data from the environment and enable real-time monitoring and analysis of the data.

4.Difference

Wireless Adhoc Network	Wireless Sensor Network
The medium used in wireless adhoc networks is radio waves.	The medium used in wireless sensor networks are radio waves, infrared, optical media.
Application independent network is used.	Application dependent network is used.
Hop-to-Hop routing takes place.	Query based (data centric routing) or location based routing takes place.
It is heterogeneous in type.	It is homogeneous in type.
The traffic pattern is point-to-point.	The traffic pattern is any-to-any, many-to-one, many-to-few, one-to-many.
Wireless router is used as an inter-connecting device.	Application level gateway is used as an inter-connecting device.
The data rate is high.	The data rate is low.
Supports common services.	Supports specific applications.
Traffic triggering depends on application needs.	Triggered by sensing events.
IP address is used for addressing.	Local unique MAC address or spatial IP is used for addressing.

UNIT – 2.

5.What are MAC protocols. Explain in detail

MAC (Media Access Control) protocols are a set of rules and procedures that govern how devices in a network access the shared communication medium, such as a wireless channel. They are responsible for coordinating the access of multiple devices to the medium in order to prevent collisions and ensure efficient use of the available bandwidth.

There are several types of MAC protocols that can be used in wireless networks, including:

Carrier Sense Multiple Access (CSMA): CSMA protocols listen to the channel before transmitting, and if the channel is busy, they wait for it to become idle before transmitting.

Time Division Multiple Access (TDMA): TDMA protocols divide the channel into time slots and assign each device a specific slot during which it can transmit. This allows multiple devices to share the channel without interfering with each other.

Code Division Multiple Access (CDMA): CDMA protocols assign each device a unique code and use spread spectrum techniques to allow multiple devices to transmit at the same time on the same channel.

Aloha: In ALOHA protocol, each device transmits whenever it has data to send, and if two or more devices transmit at the same time, a collision occurs.

Hybrid MAC: These protocols are the combination of two or more basic MAC protocols to achieve better performance

An example of a MAC protocol in action is a wireless network in a coffee shop. A number of customers are connected to the network, all trying to access the internet at the same time. The MAC protocol in use would coordinate their access to the wireless channel, allowing each device to transmit and receive data without interfering with the other devices on the network.

Overall, MAC protocols are an important aspect of wireless networking that help to ensure efficient use of the available bandwidth and prevent collisions between devices trying to access the shared communication medium.

6.Discuss the design goals of MAC protocols

The design goals of MAC protocols are to ensure efficient use of the shared communication medium and to prevent collisions between devices trying to access the medium. Some of the key design goals of MAC protocols include:

Channel Access: The MAC protocol should provide a mechanism for devices to share the channel in an efficient way. This is typically done by implementing a mechanism for devices to request access to the channel, such as carrier sensing or time-slot allocation.

Fairness: The MAC protocol should provide a mechanism for devices to have equal access to the channel, regardless of their location, power level, or data rate.

Throughput: The MAC protocol should provide a mechanism for maximizing the amount of data that can be transmitted over the channel in a given time period.

Latency: The MAC protocol should provide a mechanism for minimizing the delay between when a device requests access to the channel and when it is granted access.

Energy Efficiency: The MAC protocol should aim to minimize the energy consumed by the devices while accessing the medium, which is crucial for wireless sensor networks and other low-power applications.

Scalability: The MAC protocol should be able to handle a large number of devices without becoming inefficient or unstable.

Robustness: The MAC protocol should be able to handle network disturbances, such as interference and fading, without causing the network to fail.

Security: The MAC protocol should provide a mechanism for protecting the network from unauthorized access and malicious attacks.

Overall, the design goals of MAC protocols are to provide efficient and fair access to the shared communication medium, maximize throughput and minimize latency, energy efficiency, scalability, robustness and security.

7.What is D-PRMA? Explain in detail

D-PRMA (Distance-based Probabilistic Routing for Multi-hop Ad-hoc Networks) is a routing protocol for ad-hoc networks that uses a probabilistic approach to determine the next hop for a packet. The main goal of D-PRMA is to balance the load between the nodes and ensure that the network is stable and efficient.

In D-PRMA, each node maintains a routing table that contains information about the distance to other nodes in the network. When a node receives a packet, it uses the information in its routing table to select the next hop for the packet. The selection process is based on a probability function that takes into account the distance to the destination and the load on the neighboring nodes. This approach helps to balance the load between the nodes and ensure that the network is stable and efficient.

D-PRMA also uses a mechanism to adapt the probability function based on the network conditions. This allows the protocol to adapt to changing conditions in the network and maintain good performance.

D-PRMA has some advantages over other routing protocols:

It balances the load between the nodes and ensures that the network is stable and efficient.

It adapts the probability function based on the network conditions.

It works well in networks with a high mobility of nodes.

8.What is Leach? Explain in detail

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a routing protocol for wireless sensor networks (WSNs). It is designed to reduce energy consumption in WSNs by clustering the sensor nodes and rotating the role of cluster-head among the nodes.

In LEACH, the sensor nodes are organized into clusters, with each cluster having a single cluster-head. The cluster-head is responsible for collecting data from the other nodes in the cluster, processing the data, and transmitting it to the base station. The other nodes in the cluster, known as members, are responsible for sensing the environment and forwarding data to the cluster-head.

The key feature of LEACH is its adaptive nature, which allows it to adjust to the changing conditions in the network. The protocol periodically selects new cluster-heads and adjusts the size of the clusters based on the remaining energy of the nodes. This helps to ensure that the cluster-heads do not become overburdened and that energy is distributed evenly among the nodes.

LEACH also uses a randomized approach to cluster formation to prevent any single node from becoming a cluster head too frequently and thus conserve energy.

LEACH protocol is a hierarchical protocol that organizes the nodes into clusters and then uses a TDMA (Time Division Multiple Access) scheme for communication within the cluster. This allows for efficient use of the channel and reduces energy consumption.

9.MAC PROTOCOL ISSUES

The Medium Access Control (MAC) protocol is a sublayer of the Data Link Layer in the OSI Model that controls how devices in a network share access to a shared communication medium, such as a wireless network or Ethernet. Common issues with MAC protocols include:

Collision: When two or more devices transmit at the same time, their signals can interfere with each other, resulting in a collision. This can cause the devices to retransmit their data, leading to delays in communication.

Hidden node problem: This occurs when a device cannot hear another device's transmission because of distance or obstacles, but both devices can hear a third device. This can lead to collisions and wasted bandwidth.

Exposed node problem: This occurs when a device can hear another device's transmission but the other device cannot hear it. This can lead to wasted bandwidth and increased energy consumption.

Channel contention: This occurs when multiple devices attempt to access the same channel at the same time, leading to delays in communication and wasted bandwidth.

Limited bandwidth: In some cases, the available bandwidth may be insufficient to support the number of devices attempting to communicate. This can lead to delays in communication and dropped packets.

Overhearing: Devices may overhear packets that are not intended for them, causing unnecessary processing and increased energy consumption.

Solutions to these issues include using carrier sense multiple access (CSMA) and request to send/clear to send (RTS/CTS) protocols, using a centralized controller to manage access to the medium, and using frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) to reduce the likelihood of collisions.

10. MACAW PROTOCOL

MACAW (MAC Address with Authentication) is a security protocol that is used to authenticate devices in a network by using their MAC addresses.

The basic idea behind the MACAW protocol is that each device in a network has a unique MAC address that is used to identify it. When a device attempts to join the network, the MACAW protocol is used to authenticate the device's MAC address against a list of authorized addresses. If the address is on the list, the device is granted access to the network.

The MACAW protocol works by having a trusted source (such as an access point) broadcast a challenge to the devices in the network. Each device then responds with its MAC address and a secret key that is used to encrypt the address. The trusted source then compares the received MAC addresses with the authorized addresses and grants access to the devices whose addresses match.

This protocol is designed to be simple to implement and provides a basic level of security by preventing unauthorized devices from joining the network. However, it is also important to note that the protocol does not provide any encryption for the data transmitted over the network, so it should not be used as a standalone security solution.

Some of the main advantages of the MACAW protocol are its simplicity and low overhead, which makes it well suited for small and resource-constrained networks. However, it also has some disadvantages, such as it does not protect against spoofing or replay attacks, and also does not provide any encryption for the data transmitted over the network.

11.Contention based protocols with reverse mechanism

Contention-based protocols are a class of wireless communication protocols that allow multiple devices to share a communication channel by using a mechanism to resolve contention for the channel. A reverse mechanism is a mechanism that is used to resolve contention for the channel by allowing devices that were unsuccessful in accessing the channel to have priority over devices that were successful.

One example of a contention-based protocol with a reverse mechanism is the "Reverse CSMA/CA" (Carrier Sense Multiple Access with Collision Avoidance) protocol, which is a variation of the standard CSMA/CA protocol used in wireless networks such as IEEE 802.11. In the Reverse CSMA/CA protocol, devices that were unsuccessful in accessing the channel in the previous contention period have priority over devices that were successful. This helps to ensure that devices that were unsuccessful in accessing the channel have a higher probability of success in the next contention period.

Another example is the "Reverse TDMA" (Time Division Multiple Access) protocol, which is a variation of the standard TDMA protocol used in wireless networks. In the Reverse TDMA protocol, devices that were unsuccessful in accessing the channel in the previous time slot have priority over devices that were successful. This helps to ensure that devices that were unsuccessful in accessing the channel have a higher probability of success in the next time slot.

The reverse mechanism used in these protocols helps to improve the overall performance of the network by ensuring that devices that were unsuccessful in accessing the channel have a higher probability of success in the next contention period. This can help to reduce collisions and improve the efficiency of the network. However, the reverse mechanism can also increase the complexity of the network by requiring devices to coordinate their transmissions.

12.Low cycle

Low-duty cycle protocols are a class of wireless communication protocols that are designed to minimize energy consumption by reducing the amount of time that a device spends transmitting and receiving data. These protocols are commonly used in wireless sensor networks, where devices have limited power resources and need to operate for long periods of time without being recharged.

One example of a low-duty cycle protocol is the duty-cycled protocol. In this protocol, devices periodically wake up and listen for a short period of time (referred to as the "active period") to check if there is any data to be transmitted or received. If there is no data, the device goes back to sleep (referred to as the "sleep period") to conserve energy. The duration of the active and sleep periods can be adjusted based on the specific requirements of the network.

Another example is the Scheduled-based protocol, this protocol allows devices to schedule their transmissions and receptions in advance, thus reducing the amount of time spent listening for data.

Low-duty cycle protocols can be effective in extending the lifetime of a wireless sensor network, but they also have some disadvantages. One disadvantage is that they can increase the delay in transmitting data, since devices may not be awake to receive data at the time it is transmitted. Additionally, these protocols can increase the complexity of the network, since devices need to coordinate their sleep and wake periods.

In general, low-duty cycle protocols are best suited for networks where energy conservation is a critical requirement and the data rate is not very high.

13.The IEEE 802.11 DCF (Distributed Coordination Function) backoff mechanism

is used to prevent collisions in wireless networks that use the 802.11 standard. It is an important aspect of the 802.11 protocol that helps to improve the overall performance of the network.

When two or more devices attempt to transmit data at the same time, a collision can occur, resulting in wasted bandwidth and retransmission of data. To avoid collisions, the 802.11 DCF uses a backoff mechanism that requires devices to wait a random amount of time before attempting to transmit again. This reduces the likelihood that multiple devices will attempt to transmit at the same time, and helps to improve the efficiency of the network.

The backoff mechanism works by having devices that are ready to transmit data listen for a clear channel before attempting to send their data. If the channel is busy, the device will wait for a random amount of time before trying again. The waiting time is determined by a backoff counter, which is incremented every time the device is unsuccessful in accessing the channel.

The backoff mechanism is particularly helpful in wireless networks where there is a high degree of contention for the channel, such as in a crowded environment or in a network with many devices. By ensuring that devices wait for a random amount of time before attempting to transmit again, the backoff mechanism helps to reduce collisions and improve the overall performance of the network.

However, it should be noted that the backoff mechanism also has some disadvantages. It can cause delays in the transmission of data, and it can also increase the complexity of the network by requiring devices to coordinate their transmissions.

UNIT – 3.

14.HYBRID ROUTING PROTOCOLS

*Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR)

It is based on extracting core nodes (also called as Dominator nodes) in the network. Core nodes together approximate the minimum Dominating Set (DS).There exists at least one core node within every three hops. The path between two core nodes is termed as virtual link.

Advantages:

- Performs both routing and QoS path computation very efciently
- Utilization of core nodes reduces trafc overhead. Disadvantages
- Since route establishment is carried out at core nodes, the movement of core nodes adversely afects the performance of the protocol.
- Core node update information causes control overhead.

*Zone Routing Protocol (ZRP)

Effectively combines the best features of both Proactive and Reactive routing protocols.0 It use a Proactive routing scheme within a limited zone in the neighborhood of every node. Uses a Reactive routing scheme for nodes beyond this.

Route Establishment: When a node s has packets to be sent to a destination node0 d, it checks whether node d is within its zone.0

If the destination belongs to its own zone, then it delivers the packets directly.0 Otherwise, node s broadcasts the RouteRequest to its peripheral nodes.0 (RouteRequest to node 2, 3, 5, 7, 9, 10, 13, 14 and 15).0

If any peripheral node fnds node d to be located within its routing zone, it sends a RouteReply back to node 8 indicating the path.0

This process continues until node d is located.

Advantage0

Reduce the control overhead by combining the best features of Proactive and Reactive protocols.0

Disadvantage0

Control overhead may increase due to the large overlapping of nodes routing zones.

*Zone Based Hierarchical Link State Routing Protocol (ZHLS)

- ZHLS uses the geographical location info of the nodes to form non-overlapping zones. A Hierarchical Addressing that consists of a zone ID and a node ID is employed.
- If a source node src wants to communicate with a destination node dest, src0 checks whether dest resides in its own zone.0
- If dest belongs to same zone, then packets are delivered to the dest.
- If dest does not belong to the same zone, then the src originates a location request packet containing the sender's and destination's information. This location info is forwarded to every other zone.
- The gateway node of a zone at which the location request packet is received verifes its routing table for the destination node.

Advantages0

- Reduce storage requirements and common overhead. Non overlapping zones.

Disadvantages

- Geographical info may not be available in all environments.

15.CLASSIFICATIONS OF ROUTING PROTOCOLS

The routing protocol for ad-hoc wireless networks can be broadly classifed into 4 categories based on:

Routing information update mechanism.

Classifed into 3 major categories based on the routing information update mechanism. They are:

Proactive:

o Every node maintains the network topology information in the form of routing tables

o Whenever a node requires a path to a destination, it runs an appropriate path-fnding algorithm

Reactive:

o Do not maintain the network topology information.

o Obtain the necessary path when it is required.

Hybrid routing protocols:

o Combine the best features of the above two categories.
o For routing within this zone, a table-driven approach is used.0
o For nodes that are located beyond this zone, an on-demand approach is used.

Use of temporal information for routing

The protocols that fall under this category can be further classifed into two types :0
Routing protocols using past temporal information:0
o Use information about the past status of the links or the status of links at the time of routing to make routing decisions.0
Routing protocols that use future temporal information:0
o Use information about the about the expected future status of the wireless links to make0 approximate routing decisions.

Routing topology

Can make use of either a fat topology or a hierarchical topology for routing.

Flat topology routing protocols:

o It assumes the presence of a globally unique addressing mechanism for nodes in an ad hoc0 wireless network

Hierarchical topology routing protocols:0
o Make use of a logical hierarchy in the network and an associated addressing scheme.0 o The hierarchy could be based on geographical information.

16.HIERARCHICAL ROUTING PROTOCOLS0

The use of routing hierarchy has several advantages

Reduction in size of routing tables and better scalability.

Hierarchical State Routing (HSR) protocol0

It is a distributed multi-level hierarchical routing protocol that employs clustering at diferent levels0
with efcient membership management at every level of clustering.0 Each cluster has its leader.

Disadvantage0

Process of exchanging information concerned all the levels of the hierarchy as well as the process0
of leader election in every cluster makes it quite problematic for adhoc networks.

Fish-Eye State Routing Protocol (FSR)

- Property of a fish's eye that can capture pixel information with greater accuracy near its eye's focal point.
- Each node maintains accurate information about near nodes.0
- Nodes exchange topology information only with their neighbors.

Advantages0

Reduce bandwidth consumption by link state update packets.0
Suitable for large and highly mobile adhoc wireless network.0

Disadvantages0

Very poor performance in small adhoc networks

POWER-AWARE ROUTING PROTOCOLS

o This metric aims at minimizing the power consumed by a packet in traversing from source node to the destination node.0
o The energy consumed by a packet when traversing through a path is the sum of the energies required at every intermediate hop in that path.

Minimum cost per packet0
o In order to maximize the life of every node in the network, this routing metric is made as a0 function of the state of the node's battery.0
o A node's cost decreases with an increase in its battery change and vice versa.

17.Localization and positioning in routing protocols

Localization and positioning are important concepts in routing protocols for ad-hoc networks, as they provide information about the location of nodes in the network. This information can be used to improve the performance of the routing protocol and make it more efficient.

Localization refers to the process of determining the location of nodes in the network. This can be done using a variety of techniques, such as GPS, triangulation, or received signal strength. Once the location of a node is known, it can be used to improve the performance of the routing protocol.

Positioning, on the other hand, is the process of determining the position of a node in relation to other nodes in the network. This information can be used to improve the performance of the routing protocol by providing more accurate and efficient routes.

In routing protocols for ad-hoc networks, the use of localization and positioning information can help to improve the performance of the protocol in several ways:

- It allows for more efficient routes to be selected, as the location of the nodes is known.
- It allows for the use of geographic routing, where the routing decisions are based on the location of the nodes.
- It allows for the detection and avoidance of congestion or interference in the network.
- It enables the use of localization-based algorithms that take into account the relative positions of the nodes in the network.

18. Explain Table Driven Routing Protocol.

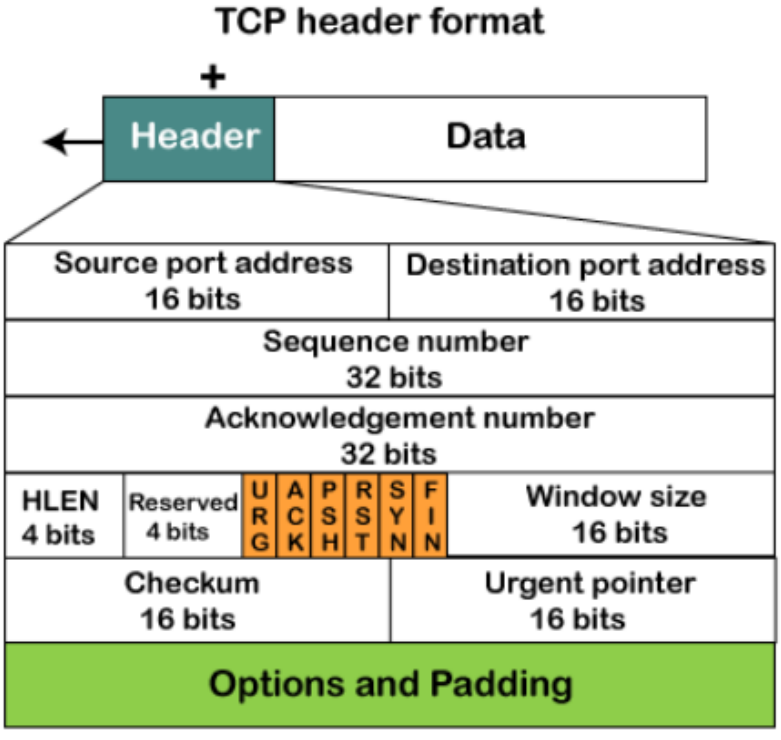
19. On Demand Routing Protocols.

20. A flooding is efficiently handled with the help of protocols.

THESE 3 QUESTIONS NEEDS TO BE SEARCHED.

UNIT 4.

21. TCP header format.



- **Source port:** It defines the port of the application, which is sending the data. So, this field contains the source port address, which is 16 bits.
- **Destination port:** It defines the port of the application on the receiving side. So, this field contains the destination port address, which is 16 bits.
- **Sequence number:** This field contains the sequence number of data bytes in a particular session.
- **Acknowledgment number:** When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received. For example, if the receiver receives the segment number 'x', then it responds 'x+1' as an acknowledgment number.
- **HLEN:** It specifies the length of the header indicated by the 4-byte words in the header. The size of the header lies between 20 and 60 bytes. Therefore, the value of this field would lie between 5 and 15.
- **Reserved:** It is a 4-bit field reserved for future use, and by default, all are set to zero.
- **Flags**
  There are six control bits or flags:

  1. **URG:** It represents an urgent pointer. If it is set, then the data is processed urgently.
  2. **ACK:** If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.

3. **PSH:** If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.
4. **RST:** If it is set, then it requests to restart a connection.
5. **SYN:** It is used to establish a connection between the hosts.
6. **FIN:** It is used to release a connection, and no further data exchange will happen.

- **Window size**
  It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment. The value of this field is determined by the receiver.
- **Checksum**
  It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.
- **Urgent pointer**
  It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.
- **Options**
  It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.

22. ACTP

APPLICATION CONTROLLED TRANSPORT PROTOCOL0

- It is a light-weight transport layer protocol.0
- Assigns the responsibility of ensuring reliability to the application layer.0
- ACTP stands in between TCP and UDP where TCP experiences low performance with high reliability and UDP provides better performance with high packet loss in Adhoc wireless networks.
- Delivery status is maintained at the ACTP layer. This reflect Successful delivery of the packet.
- A possible loss of the packet
- Remaining time for the packet
- No state information exists at the ACTP layer Disadvantage:
- Not compatible with TCP

Application Controlled Transport Protocol is a type of transport protocol that is controlled by the application, rather than the operating system or network stack. This means that the application has direct control over the flow of data across the network, rather than relying on the underlying network stack to handle network communication.

The main advantage of an Application Controlled Transport Protocol is that it provides more fine-grained control over the flow of data, allowing the application to optimize communication for its specific requirements. This can lead to improved performance, reliability, and security compared to traditional transport protocols, which may not be designed with specific applications in mind.

For example, an application that requires low latency and high throughput might use an Application Controlled Transport Protocol to prioritize and optimize the flow of data across the network. This could include features such as congestion control, error correction, and flow control to ensure that data is delivered quickly and reliably.

Another example might be an application that needs to securely send data across the network. In this case, the Application Controlled Transport Protocol might provide encryption, authentication, and data integrity features to ensure that the data is protected as it travels over the network.

Overall, Application Controlled Transport Protocols provide a high degree of flexibility and control for applications, allowing them to optimize communication for their specific requirements and improve overall performance, reliability, and security.

Regenerate response.

23. PERFORMANCE OF TCP IN AD HOC

TCP does not perform well in Adhoc wireless network

1. Misinterpretation of packet loss:

In traditional TCP design, the packet loss is mainly attributed to network congestion.

Ad hoc wireless network experience a much higher packets loss due to0 High bit rate

2.Uni directional path:0

TCP relies on end-to-end ACK for ensuring reliability. Path break on an entirely different reverse path can affect the performance of the network

3.Multipath Routing:

For TCP, multipath routing leads to signifcant amount of out of order packets.

4.The use of sliding window based transmission:0

TCP uses a sliding window for fow control.

This can contribute to degraded performance in bandwidth constrained ad hoc wireless network.

5.Frequent path breaks:

If the route re-establishment time is greater than the RTO period of TCP sender, then the TCP sender. assumes congestion in the n/w ,retransmits lost packets and initiates congestion control algorithm.0

This leads to wastage of bandwidth and battery power.

24. ISSUE AND DESIGN GOALS OF TCP

Issue: Same as Q6.

DESIGN GOALS OF TCP:

- It should incur minimum connection set up and connection maintenance overheads.0
- It should have mechanisms for congestion control and fow control in the network.0
- It should be able to provide both reliable and unreliable connections as per the requirements of the application layer.
- It should be able to adapt to the dynamics of the network such as rapid changes in topology.
- Bandwidth must be used efciently.
- It should be aware of resource constraints such as battery power and bufer sizes and make efcient use of them.
- It should have a well-defned cross-layer interaction framework.

25. Issues in routing protocols ELFN approach (Explicit Link Failure Notifications).

The Explicit Link Failure Notifications (ELFN) approach is a technique used in routing protocols to detect and respond to link failures in a network. However, it also has some issues that can affect the performance and stability of the network:

Overhead: ELFN approach requires routers to send explicit link failure notifications (ELFNs) to their neighbors when a link failure is detected, this can increase the amount of control messages sent in the network, which can cause network congestion and reduce the efficiency of the network.

Convergence time: ELFN approach can have a longer convergence time compared to other link failure detection methods, as it relies on explicit notifications of link failure to update routing tables, which may take longer than other methods such as hello protocol or keepalives.

Scaling: ELFN approach may not scale well in large networks, since the number of ELFN messages sent increases with the number of nodes in the network, this can cause network congestion and reduce the efficiency of the network.

Security: ELFN approach does not provide any security mechanism to protect the network from malicious nodes, an attacker can inject false ELFN messages to disrupt the network, this can cause network instability and reduce the availability of the network.

Complexity: ELFN approach can increase the complexity of the routing protocol as it requires the implementation of additional mechanisms to handle ELFN messages, this can increase the development and maintenance costs of the network.

26.TCP FEEDBACK

FEEDBACK BASED TCP (TCP – F)0

Improves performance of TCP.0

Uses a feedback based approach.0

- The routing protocol is expected to repair the broken path within a reasonable time period
- In TCP-F, an intermediate node, upon detection of a path break, sends route failure notifcation (RFN) packet. This intermediate node is called Failure point (FP).0 This RFN packet is routed toward the sender of the TCP session.0
- If any intermediate nodes that receive RFN has an alternate route to the same destination, then it discards the RFN packet and uses the alternate path for forwarding further data packets.
- When TCP sender receives an RFN packet, it goes into a state called snooze. In this state, a sender.
- Stops sending any more packets to the destination.0 o Cancels all timers.
- When route failure timer expires, the TCP sender changes from snooze state to connected state.0
- When the route re-establishment has been done, then the failure point sends Route Re-establishment.
- Notifcation (RRN) packet to the sender and the TCP state is updated back to the connected state.

ELFN

TCP WITH EXPLICIT LINK FAILURE NOTIFICATION: (TCP-ELFN)

Improves TCP performance in adhoc wireless network.

Similar to TCP-F.

ELFN is originated by the node detecting a path break

upon detection of a link failure to the TCP sender.0

This can be implemented in two ways :0

1. By sending an ICMP Destination Unreachable (DUR) message to the sender.0 (or)0
2. By piggy-backing this information to the sender.0

Once the TCP sender receives the ELFN packet, it disables its retransmission timers and enters a standby state.0

In this state, it periodically originates probe packets to see if a new route is established.0

Upon reception of an ACK by the TCP receiver for the probe packets, it leaves the standby state, and continues to function as normal.